DIGITAL FORENSICS MYANMAR

Low Budget, High Impact Digital Forensics Investigation

Aung Zaw Myo

6/3/2025

ယခု PDF သည် Digital Forensics ကိုစိတ်ပါဝင်စားသည့် လူတစ်ဦးတစ်ယောက် (သို့မဟုတ်) အဖွဲ့အစည်းများက Digital Forensics Lab တစ်ခုကို ကုန်ကျစာရိတ် သက်သာစွာဖြင့် တည်ထောင်လုပ်ကိုင်နိုင်ရန်အတွက် Reference ပြုလုပ်နိုင်ရန်ဖြစ်ပါသည်။ တစ်ခုချင်းစီကို ဘယ်လိုအသုံးပြုရမလဲဆိုတာကိုမဖော်ပြထားပါ။

ယနေ့ခေတ်အခြေအနေအရ လူတိုင်းနီးပါးမှာ Digital Device , Banking Application, Sim Card, Social Network, Messaging Application အနည်းဆုံးတစ ခို ှိုလာနေပြီဖြစ်ပါတယ်။ ယခင်က Case တစ်ခုဖြစ်ရင် လက်ဗွေတွေ၊ ခြေရာတွေက အရေးပါတဲ့နေရမှာပါဝင်သလို ဒီနေ့ခေတ်မှာတော့ အပေါ်မှာပြောခဲ့တဲ့ Digital Device, Etc … တွေက လက်ဗွေတွေ၊ ခြေရာတွေလိုပဲ အရေးပါတဲ့နေရာ ကနေပါဝင်လာပါတယ်။ ဥပမာ လူတစ်ယောက်က အိမ်မှာရှိတယ်လို့ဘယ်လိုပဲပြောပြော သူ့ဖုန်းကို Analysis လုပ်လိုက်ရင် အိမ်ထဲမှာ ရှိတဲ့ အချိန်မှာ Phone Bluetooth က ကားထဲမှာရှိတဲ့ Bluetooth နဲ့ချိတ်ဆက်နေတာမျိုး၊ အဲဒီထက်ပိုရင် သူအသုံးပြုတဲ့ Phone Sim Card က အိမ်နားမှာရှိတဲ့ Cell Tower နဲ့ချိတ်ဆက်မနေပဲ အိမ်ကနေ သူသွားတဲ့ လမ်းတလျောက်မှာရှိတဲ့ Cell Tower တွေနဲ့ချိတ်ဆက်ခဲ့တာမျိုး အခြားနေရာမှာရှိတဲ့ Cell Tower နဲ့ချိတ်ဆက်ခဲ့တဲ့ (Cell Routing Information) စတာတွေနဲ့ Analysis ပြုလုပ်နိုင်ပါတယ်။

Open Source vs. Commercial Software: Pros and cons

Open Source Cons:

- Open Source ဖြစ်တာကြောင့် အခမဲ့အသုံးပြုနိုင်ခြင်း။
- မိမိကျွမ်းကျင်မှုရှိလျင် စိတ်ကြိုက်ပြင်ဆင်အသုံးပြုနိုင်ခြင်း။
- Popular ဖြစ်တဲ့ Open Source တွေဆိုလျင် Community Forum & Tutorial များရှိခြင်း / Update များပြုလုပ်နိုင်ခြင်း။

Open Source Pros:

- Commercial Tools တွေလို push-button forensics မဟုတ်တာကြောင့် အသုံးပြုသူမှ ကျွမ်းကျင်မှုရှိရန်လိုအပ်ခြင်း။
- Commercial Software များလို Support မရှိခြင်း။

- Update များကို တစ်ခါတစ်ရံမှသာ ရနိုင်ခြင်း/ လုံးဝမရရှိခြင်း။

Commercial Software: Cons

- push-button forensics ဖြစ်တာကြောင့် ကအသုံးပြုရတာလွယ်ကူခြင်း။
- နားလည်တာ/ မရနိုင်တာကို Support သို့အချိန်မရွေးမေးမြန်းနိုင်ခြင်း။
- Result များကို စိတ်ချယုံကြည်နိုင်ခြင်း။
- Update / Bug Fix တွေကို ရရှိနိုင်ခြင်း။

Commercial Software: Cons

- နှစ်စဉ်လိုင်စင် စရိတ်မြင့်မားခြင်း။
- push-button forensics ဖြစ်တာကြောင့် Result ရဖို့ ဘာတွေစစ်ဆေးတာလဲဆိုတာကို မသိနိုင်ခြင်း။
- မိမိစိတ်ကြိုက်ပြင်ဆင်အသုံးမပြုနိုင်ခြင်း။

Open Source သုံးရမလား Commercial Software သုံးရမလားဆိုတာကတော့ ကိုယ်တတ်နိုင်တဲ့ ငွေပမာဏ၊ နည်းပညာကျွမ်းကျင်မှုတို့အပေါ်မူတည်ပြီး ရွေးချယ်နိုင်ပါတယ်။ Commercial Computer Forensics / Mobile Forensics Tools များကလဲ Popular ဖြစ်တဲ့ Open Source များအပေါ်အခြေခံပြီးပြုလုပ်ထားတာဖြစ်ပါတယ်။ Open Source + Commercial Software အနေနဲ့လဲ ပေါင်းစပ်အသုံးပြုနိုင်ပါတယ်။ Computer တစ်လုံးကိုပဲ Commercial Software ၂ မျိုးနဲ့ Analysis လုပ်မယ်ဆိုရင် ရရှိတဲ့ Results တွေက တူညီမှုရှိနိုင်မှာ မဟုတ်ပါဘူး။ Software A မှာမရတာကို Software B မှာရှိနိုင်သလို။ Software A/B မှာရောမရရှိနိုင်တာဖြစ်နိုင်ပါတယ်။ Software A/B မှာမရရှိတာကို Open Source မှာရရှိနိုင်တာလဲ ဖြစ်နိုင်ပါတယ်။ Forensics Commercial Tools တော်တော်များများက Open Source တွေကို အခြေခံထားတာဖြစ်ပါတယ်။ အချို့နိုင်ငံများမှာတော့ Cross Check အနေနဲ့ Product 2 မျိုး ဒါမှမဟုတ် Open Source Tools တွေကိုအသုံးပြုကြပါတယ်။

Budgeting Basics

ကိုယ် Lab အနေနနဲ့တည်ဆောက်မည့် Lab က ဘာကိုဦးစားပေးအနေနဲ့ ပြုလုပ်မလဲ ဆိုတဲ့အချက်ကို ဦးစားပေးစဉ်းစားရပါမယ်။ Computer (Or) Mobile Forensics ? Software တွေက Commercial (Or) Open Source ? ဘယ်အရာကိုပဲ Target ထားထား အခြေခံအကျဆုံးက အသုံးပြုမည့် Hard Ware လိုအပ်ချက်ဖြစ်ပါတယ်။ အသုံးပြုသူက သူအသုံးပြုချင်သလိုအသုံးပြုထားတဲ့ Digital Device တစ်ခုကို အချိန်တိုတိုနဲ့ Analysis ပြုလုပ်ချင်တယ်ဆိုရင် Analysis လုပ်တဲ့ Computer က Forensics Work Station မဟုတ်ရင်တောင် Performance အသင့်အတင့်ရှိတဲ့ ကွန်ပျူတာဖြစ်သင့်ပါတယ်။ နောက်တစ်ခုက Storage Requirement ဖြစ်ပါတယ်။ အခုခေတ်မှာ Mobile Phone တစ်လုံးရဲ့ Storage Size က 128 GB ဖြစ်နေပါပြီ။ အဲဒီတော့ Performance အတွက် Computer မှာ SSD အသုံးပြုပြီး Evidence Storage အတွက် Budget အနေအထားအရ သီးခြား SSD, HDD, Or NAS OR SAN ရွေးချယ်နိုင်ပါသည်။ RAM 32GB/ VGA 2 GB လောက်တော့ရှိသင့်ပါတယ်။ Storage Device တွေအတွက် အခြေခံစစ်ဆေးနည်းကို အောက်မှာဖော်ပြထားတဲ့ Link ကနေကြည့်နိုင်ပါတယ်။

eCDFP Data Acquisition

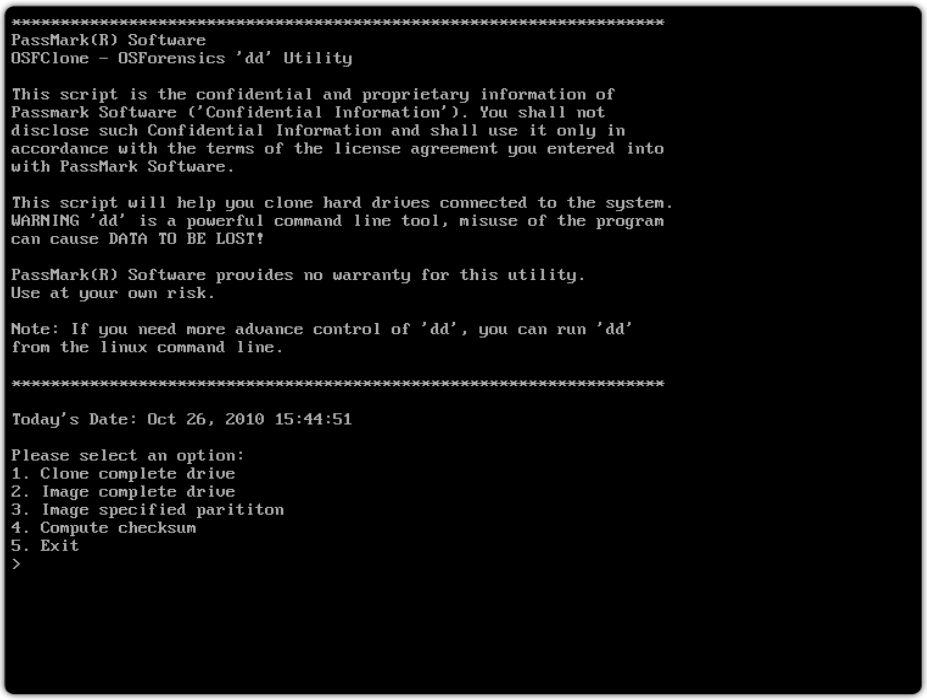
- https://www.forensicsmyanmar.com/search/label/eCDFP%20%28Moudle-2%29
- https://archive.org/details/Digital-Forensics-FTK-AZM

Disk Acquisition နဲ့ပတ်သတ်ပြီး ပြည်ပ အဖွဲ့အစည်းများအသုံးပြုနေတဲ့ Hardware Unit များကို အောက်မှာဖော်ပြထားပါတယ်။

- https://atola.com/products/tf1/simultaneous-imaging.html
- https://www.dataexpert.eu/products/forensic-hardware-tableauopentext

Disk Acquisition ကို Open Source Software အနေနဲ့အသုံးပြုနိုင်တာတွေကို အောက်မှာ ဖော်ပြထားပါတယ်။ ဖော်ပြရာမှာ Frequently Update ဖြစ်တာနဲ့ Popular ဖြစ်တဲ့ Open Source တွေကို ဦးစားပေးဖော်ပြမှာဖြစ်ပါတယ်။ (စမ်းသပ်မှုတွေအရ OSF Clone က ပိုမြန်ပါတယ်။)

- https://www.osforensics.com/tools/create-disk-images.html
- https://www.osforensics.com/tools/mount-disk-images.html
- https://www.osforensics.com/tools/write-usb-images.html
- https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81
- https://sumuri.com/software/paladin/


PassMark(R) Software
OSFClone - OSForensics 'dd' Utility
This script is the confidential and proprietary information of
Passmark Software ('Confidential Information'). You shall not
disclose such Confidential Information and shall use it only in
accordance with the terms of the license agreement you entered into
with PassMark Software.
This script will help you clone hard drives connected to the system.
WARNING 'dd' is a powerful command line tool, misuse of the program
can cause DATA TO BE LOST!
PassMark(R) Software provides no warranty for this utility.
Use at your own risk.
Note: If you need more advance control of 'dd', you can run 'dd'
from the linux command line.
Today's Date: Oct 26, 2010 15:44:51
Please select an option:
1. Clone complete drive
2. Image complete drive
3. Image specified parititon
4. Compute checksum
5. Exit
>

OSF Clone

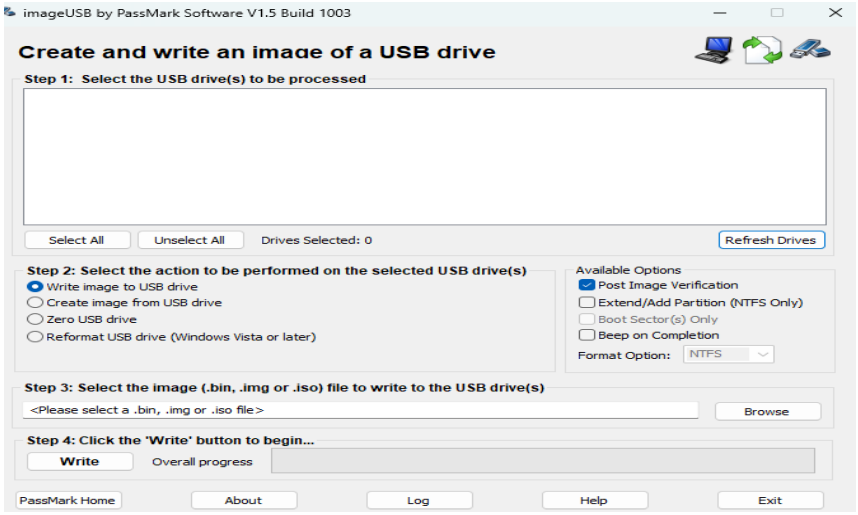
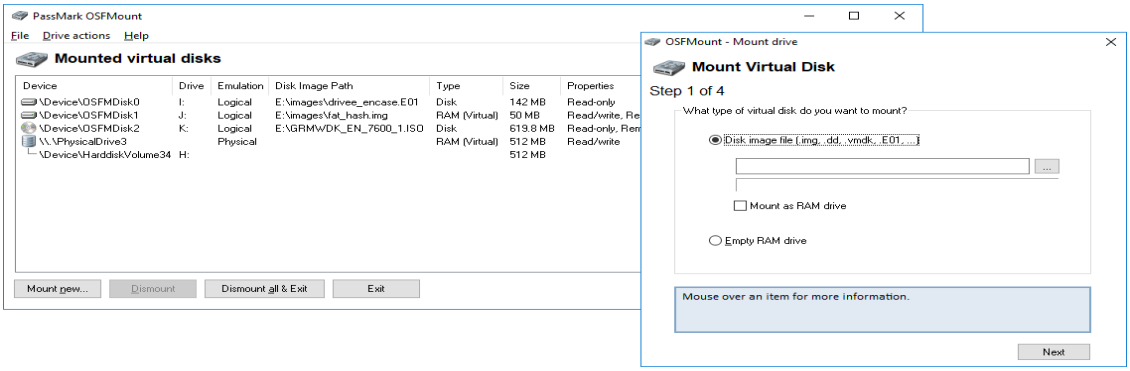
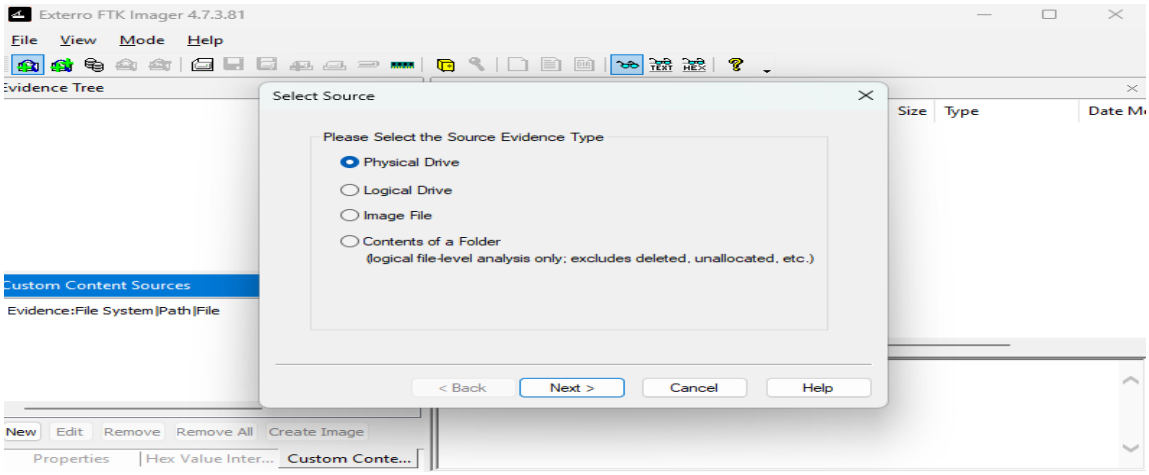

imageUSB by PassMark Software V1.5 Build 1003
Create and write an image of a USB drive
Step 1: Select the USB drive(s) to be processed
Select All
Unselect All
Drives Selected: 0
Refresh Drives
Step 2: Select the action to be performed on the selected USB drive(s)
Write image to USB drive
Create image from USB drive
Zero USB drive
Reformat USB drive (Windows Vista or later)
Available Options
Post Image Verification
Extend/Add Partition (NTFS Only)
Boot Sector(s) Only
Beep on Completion
Format Option:
NTFS
Step 3: Select the image (.bin, .img or .iso) file to write to the USB drive(s)
<Please select a .bin, .img or .iso file>
Browse
Step 4: Click the 'Write' button to begin...
Write
Overall progress
PassMark Home
About
Log
Help
Exit

Image To USB



OSFMount

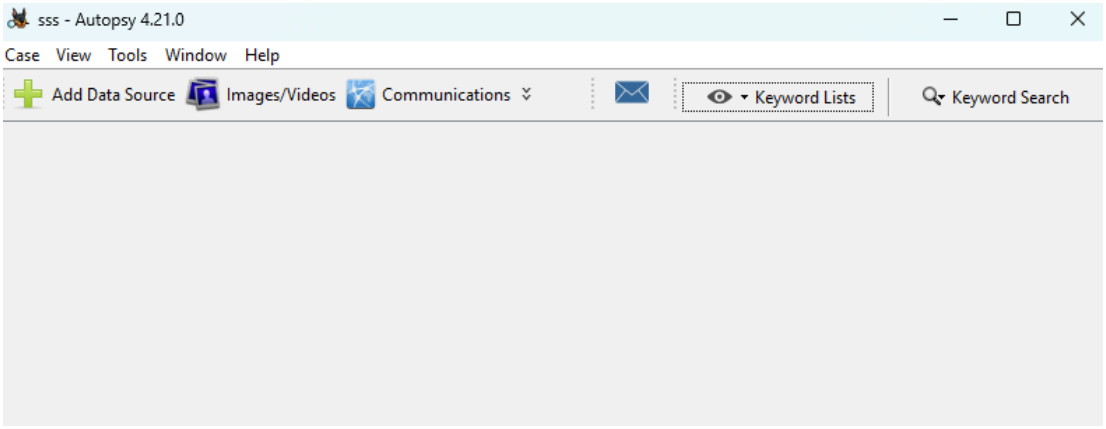


FTK Imager

Computer Forensics Open Source Tools

Autopsy ကတော့ သိတဲ့သူတော်တော်များများမှာပါ Window / Mac/ Linux File System တော်တော်များများကို စစ်ဆေးနိုင်ပါတယ်။ ကိုယ်လိုအပ်တဲ့ Investigation Module ကိုပဲရွေးချယ်ပြီးစစ်ဆေးမယ်ဆိုရင် အချိန်ပိုမြန်ပါတယ်။ IPED ကလဲပုံစံတူဖြစ်ပေမဲ့ Autopsy ကတော့ ပိုပြီး လူသုံးများပါတယ်။

- http://www.sleuthkit.org/index.php (Window/Mac/Linux)



Paladin LTS ၊ Paladin Edge 32/64

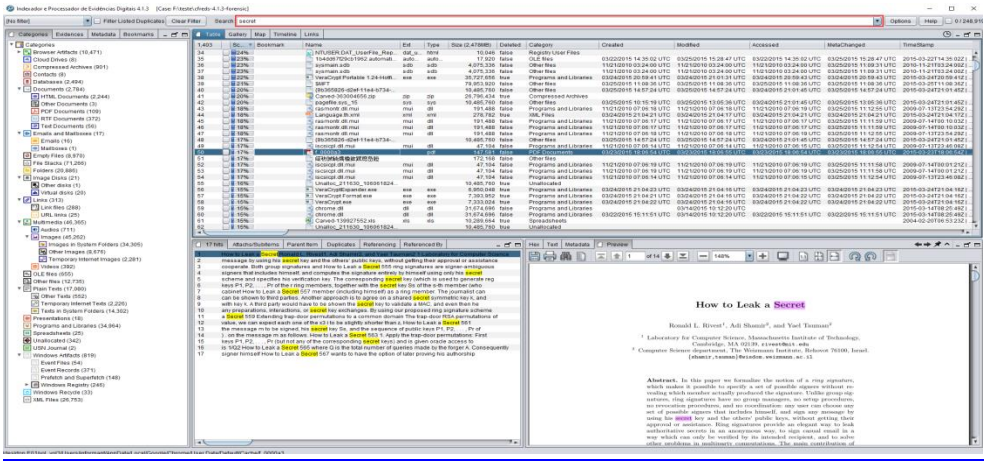
Free အနေနဲ့လဲအသုံးပြုလို့ရ လက်တွေ့ မှာ အသုံးဝင်နိုင်တာက Paladin LTS ၊ Paladin Edge 32/64ဖြစ်ပါတယ်။ Free အနေနဲ့ သုံးဖို့ အကောင့်တစ်ခု ပြုလုပ်ပြီး Visa , Master Card တစ်ခုလိုအပ်ပါတယ်။ (ငွေမဖြတ်ပါဘူး Verify ဖြစ်အောင်လုပ်တဲ့သဘောပါ)US 25 အနည်းဆုံးပေးရပါတယ် တစ်ကယ်တန်း Commercial အတွက် ဒါပေမဲ့ သိပ်မကွာပါဘူး။ ဒါနဲ့ စစ်ရင် စစ်ဆေးတဲ့ ရလဒ်ကို License ဖြစ်လို့ Sumuri မှ အာမခံတယ်ဆိုတဲ့သဘောပါ။ Paladin LTS ကိုတော့ Triage အနေနဲ့ရော Acquisition အနေနဲ့ပါ အသုံးချနိုင်ပါတယ်။ Paladin LTE မှာ Live Boot တက်ပြီး စစ်ဆေးဖို့ Autopsy ပါဝင်ပါတယ်။အခြား Open Source Tools တွေလဲပါဝင်ပါတယ်။Paladin Edge 32/64 ကတော့ Acquisition အတွက် သီးသန့်ဖြစ်ပါတယ်။

Live Boot ဖြစ်တဲ့အတွက် Secure Boot, T2, FileValue ထည့်ထားရင်တော့ သုံးလို့မရပါဘူး။ 3 ခုစလုံးကို Multi Boot လုပ်ထားပြီး အသုံးပြုလို့ရပါတယ်။ Paladin LTS တစ်ခုနဲ့တင် ရပါတယ် တစ်ကယ်ဆို သူမှာက Acquisition အတွက် နည်းလမ်းပိုစုံလင်ပါတယ်။ 3 ခုစလုံးက Ubuntu ကို Modified လုပ်ထားတာဖြစ်ပါတယ်။ Linux Command နဲ့ အကျွမ်းမဝင်တဲ့ သူတွေအတွက် သီးသန့်ပြုလုပ်ထားတာဖြစ်ပါတယ်။ Window, Mac တွေမှာ Password မသိပဲ စစ်ဆေးဖို့ကြုံလာတဲ့အခါ။ Storage ကို Acquisition (သို့မဟုတ်) Storage ကို ဖြုတ်လို့မလွယ်တဲ့အခါမျိုးမှာ အသုံးပြုနိုင်ပါတယ်။ Triage သို့မဟုတ် Acquisition အတွက် ရည်ရွယ်တာဖြစ်ပါတယ်။

- https://sumuri.com/software/paladin/

Paladin LTSC

- https://github.com/sepinf-inc/IPED



IPED

Window Forensics Artifacts

Commercial Tools နဲ့အပေါ်က Autopsy, IPED မှာအချို့သော Artifacts တွေကိုရှာမတွေ့ဘူး အဖြေထုတ်မပေးဘူးလို့ယူဆရင် ဒါမှမဟုတ် Cross Check လုပ်ဖို့လိုအပ်မယ်ထင်ရင် Window Forensics အတွက် EZ Tools နဲ့ Manual လုပ်နိုင်ပါတယ်။ ကျွန်တော် အတိုချုပ်မြန်မာလိုရေးထားတဲ့ PDF စာအုပ်ရယ် SAN & EZ Tools Poster & Ebook ကိုအောက်က Link တွေမှာ Download ပြုလုပ်နိုင်ပါတယ်။

EZ Tools Download

- https://ericzimmerman.github.io/#!index.md

EZ Tools Myanmar Ebooks Download

- https://archive.org/details/window-forensics-with-ez-tools-1-2-aung-zaw-my

EZ Tools Poster Download

- https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt60911bacd0076d64/649c897c13bff842b82ed53c/SANS_EZ-Tools_Poster.pdf

EZ Tools Cheat Sheet Download

- https://www.sans.org/posters/eric-zimmerman-tools-cheat-sheet/

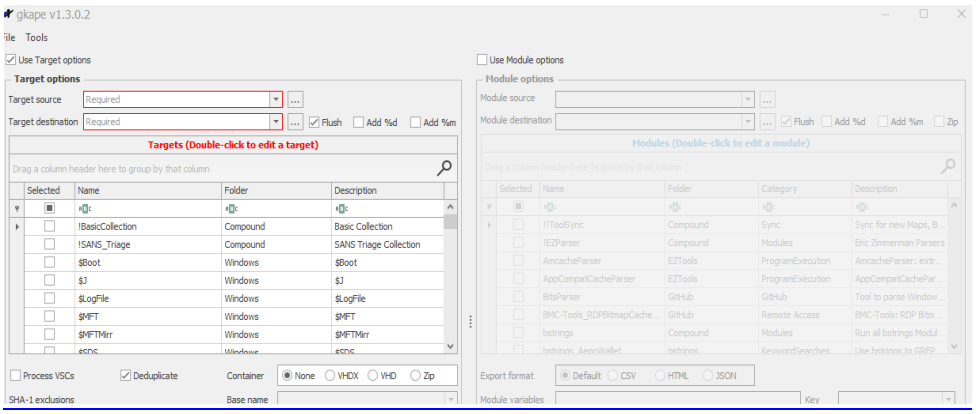
Window Registry & Window Forensics Poster Download

- https://github.com/nisargsuthar/RegistryForensicsCheatSheet
- https://www.sans.org/posters/windows-forensic-analysis
- https://www.sans.org/posters/macos-ios-forensic-analysis/

EZ Tools GUI Version Download

Digital Forensics & Incident Response အတွက် EZ Tools ကို GUI အနေနဲ့ အသုံးပြုချင်တယ်ဆိုရင် Kape ကိုအသုံးပြုနိုင်ပါတယ်။

- https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

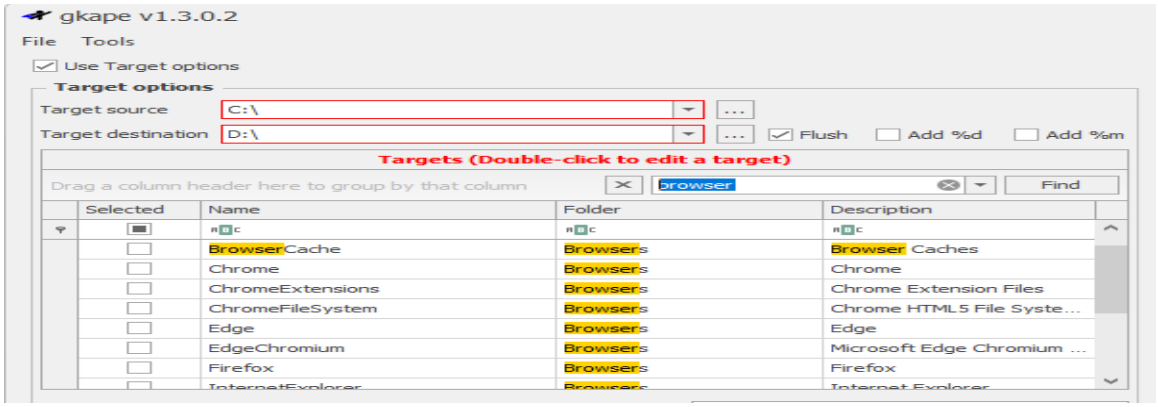


gKape

Browser Forensics

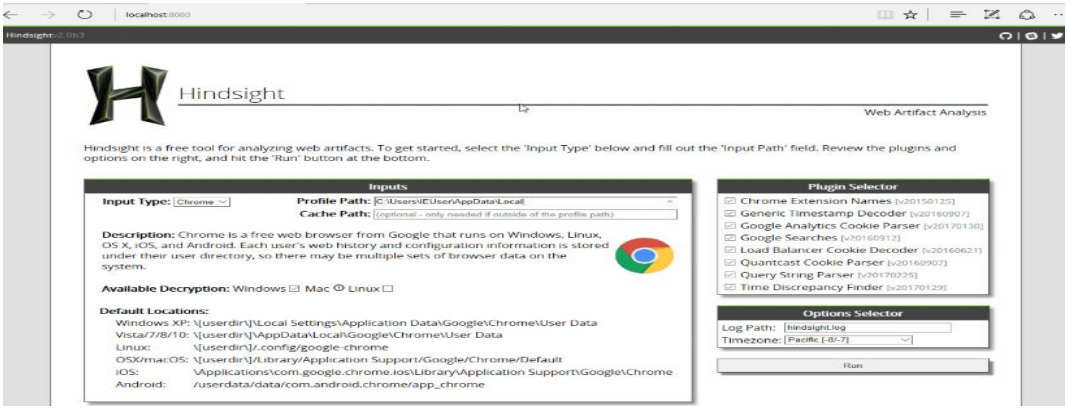
Commercial Tools တွေထဲမှာ Browser Forensics အတွက်ပဲ သီးသန့် အဖြေထုတ်ပေးတဲ့ Tools တွေရှိပါတယ်။ Open Source အနေနဲ့သုံးမယ်ဆိုရင် အောက်မှာဖော်ပြထားတဲ့ Tools တွေကနေ အသုံးပြုနိုင်ပါတယ်။ အရင်ကရေးခဲ့တဲ့ Browser Forensics Myanmar Version ကိုလဲ လေ့လာလို့ရအောင် Link ပေးထားပါတယ်။

- https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape



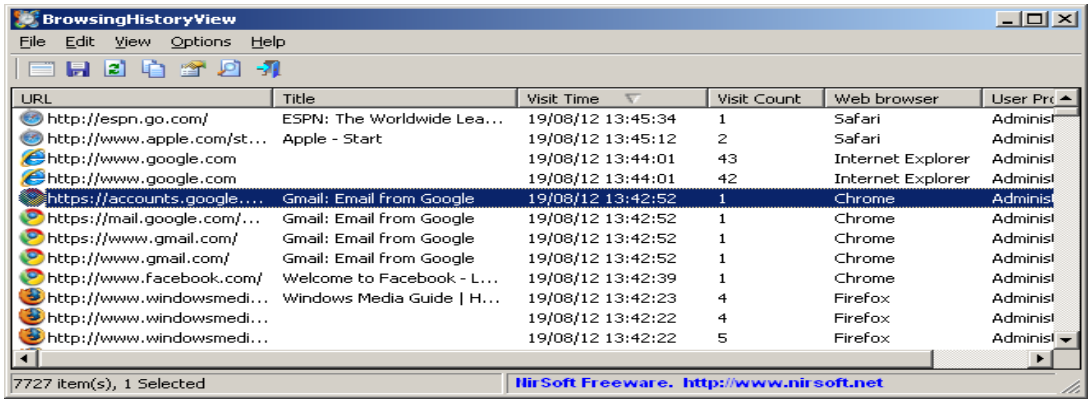
Gkape

- https://github.com/obsidianforensics/hindsigh


Hindsight
Web Artifact Analysis
Hindsight is a free tool for analyzing web artifacts. To get started, select the 'Input Type' below and fill out the 'Input Path' field. Review the plugins and options on the right, and hit the 'Run' button at the bottom.
Inputs
Input Type: Chrome
Profile Path:
Cache Path:
Description: Chrome is a free web browser from Google that runs on Windows, Linux, OS X, iOS, and Android. Each user's web history and configuration information is stored under their user directory, so there may be multiple sets of browser data on the system.
Available Decryption: Windows Mac Linux
Default Locations:
Windows XP: \[userdir\]\Local Settings\Application Data\Google\Chrome\User Data
Vista/7/8/10: \[userdir\]\AppData\Local\Google\Chrome\User Data
Linux: \[userdir\]/.config/google-chrome
OSX/macOS: \[userdir\]/Library/Application Support/Google/Chrome/Default
iOS: \Applications\com.google.chrome.ios\Library\Application Support\Google\Chrome
Android: /userdata/data/com.android.chrome/app_chrome
Plugin Selector
Chrome Extension Names
Generic Timestamp Decoder
Google Analytics Cookie Parser
Google Searches
Load Balancer Cookie Decoder
Quantcast Cookie Parser
Query String Parser
Time Discrepancy Finder
Options Selector
Log Path: hindsight.log
Timezone: Pacific [-8/-7]
Run

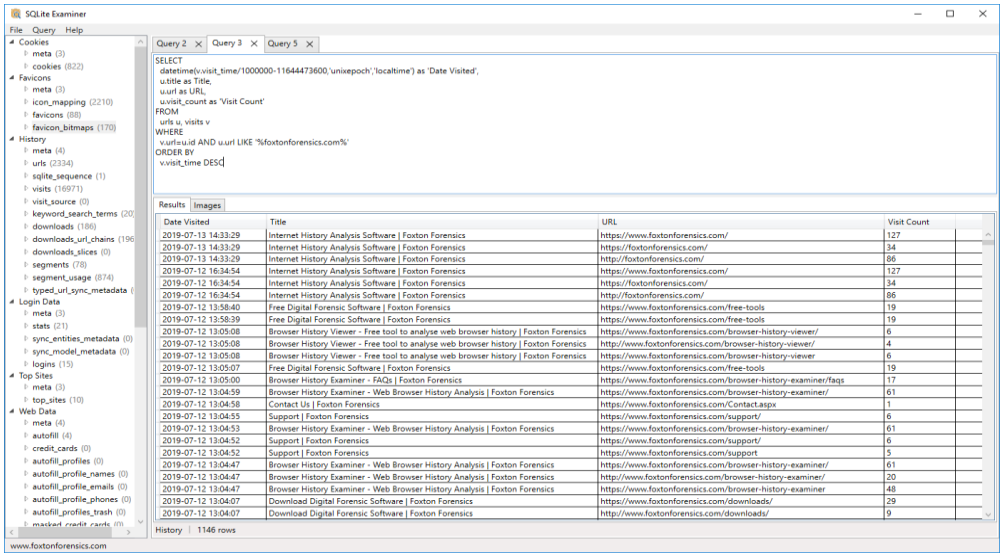
hindsigh

- https://www.nirsoft.net/web_browser_tools.html


BrowsingHistoryView
File Edit View Options Help
URL | Title | Visit Time | Visit Count | Web browser | User Pr
http://espn.go.com/ | ESPN: The Worldwide Lea... | 19/08/12 13:45:34 | 1 | Safari | Administ
http://www.apple.com/st... | Apple - Start | 19/08/12 13:45:12 | 2 | Safari | Administ
http://www.google.com | | 19/08/12 13:44:01 | 43 | Internet Explorer | Administ
http://www.google.com | | 19/08/12 13:44:01 | 42 | Internet Explorer | Administ
https://accounts.google.... | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ
https://mail.google.com/... | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ
https://www.gmail.com/ | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ
http://www.gmail.com/ | Gmail: Email from Google | 19/08/12 13:42:52 | 1 | Chrome | Administ
http://www.facebook.com/ | Welcome to Facebook - L... | 19/08/12 13:42:39 | 1 | Chrome | Administ
http://www.windowsmedi... | Windows Media Guide | H... | 19/08/12 13:42:23 | 4 | Firefox | Administ
http://www.windowsmedi... | | 19/08/12 13:42:22 | 4 | Firefox | Administ
http://www.windowsmedi... | | 19/08/12 13:42:22 | 5 | Firefox | Administ
7727 item(s), 1 Selected
NirSoft Freeware. http://www.nirsoft.net

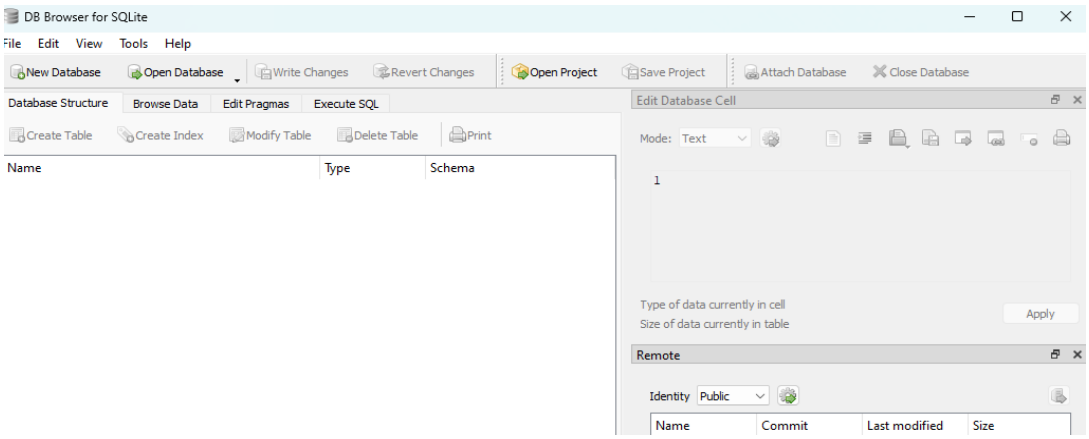
Browsing History View

- https://www.foxtonforensics.com/browser-history-viewer/
- https://www.foxtonforensics.com/browser-history-capturer/
- https://www.foxtonforensics.com/sqlite-database-examiner/


SQLite Examiner
File Query Help
Query 2 Query 3 Query 5
SELECT
datetime(v.visit_time/1000000-11644473600,'unixepoch','localtime') as 'Date Visited',
u.title as Title,
u.url as URL,
u.visit_count as 'Visit Count'
FROM
urls u, visits v
WHERE
v.url=u.id AND u.url LIKE '%foxtonforensics.com%'
ORDER BY
v.visit_time DESC
Results Images
Date Visited | Title | URL | Visit Count
2019-07-13 14:33:29 | Internet History Analysis Software | Foxton Forensics | https://www.foxtonforensics.com/ | 127
2019-07-13 14:33:29 | Internet History Analysis Software | Foxton Forensics | https://foxtonforensics.com/ | 34
2019-07-13 14:33:29 | Internet History Analysis Software | Foxton Forensics | http://foxtonforensics.com/ | 86
2019-07-12 16:34:54 | Internet History Analysis Software | Foxton Forensics | https://www.foxtonforensics.com/ | 127
2019-07-12 16:34:54 | Internet History Analysis Software | Foxton Forensics | https://foxtonforensics.com/ | 34
2019-07-12 16:34:54 | Internet History Analysis Software | Foxton Forensics | http://foxtonforensics.com/ | 86
2019-07-12 13:58:40 | Free Digital Forensic Software | Foxton Forensics | https://www.foxtonforensics.com/free-tools | 19
2019-07-12 13:58:39 | Free Digital Forensic Software | Foxton Forensics | https://www.foxtonforensics.com/free-tools | 19
2019-07-12 13:05:08 | Browser History Viewer - Free tool to analyse web browser history | Foxton Forensics | https://www.foxtonforensics.com/browser-history-viewer/ | 6
2019-07-12 13:05:08 | Browser History Viewer - Free tool to analyse web browser history | Foxton Forensics | http://www.foxtonforensics.com/browser-history-viewer/ | 4
2019-07-12 13:05:08 | Browser History Viewer - Free tool to analyse web browser history | Foxton Forensics | https://www.foxtonforensics.com/browser-history-viewer | 6
2019-07-12 13:05:07 | Free Digital Forensic Software | Foxton Forensics | https://www.foxtonforensics.com/free-tools | 19
2019-07-12 13:05:00 | Browser History Examiner - FAQs | Foxton Forensics | https://www.foxtonforensics.com/browser-history-examiner/faqs | 17
2019-07-12 13:04:59 | Browser History Examiner - Web Browser History Analysis | Foxton Forensics | https://www.foxtonforensics.com/browser-history-examiner/ | 61
2019-07-12 13:04:58 | Contact Us | Foxton Forensics | https://www.foxtonforensics.com/Contact.aspx | 1
2019-07-12 13:04:55 | Support | Foxton Forensics | https://www.foxtonforensics.com/support/ | 6
2019-07-12 13:04:53 | Browser History Examiner - Web Browser History Analysis | Foxton Forensics | https://www.foxtonforensics.com/browser-history-examiner/ | 61
2019-07-12 13:04:52 | Support | Foxton Forensics | https://www.foxtonforensics.com/support/ | 6
2019-07-12 13:04:52 | Support | Foxton Forensics | https://www.foxtonforensics.com/support | 5
2019-07-12 13:04:47 | Browser History Examiner - Web Browser History Analysis | Foxton Forensics | https://www.foxtonforensics.com/browser-history-examiner/ | 61
2019-07-12 13:04:47 | Browser History Examiner - Web Browser History Analysis | Foxton Forensics | http://www.foxtonforensics.com/browser-history-examiner/ | 20
2019-07-12 13:04:47 | Browser History Examiner - Web Browser History Analysis | Foxton Forensics | https://www.foxtonforensics.com/browser-history-examiner | 48
2019-07-12 13:04:07 | Download Digital Forensic Software | Foxton Forensics | https://www.foxtonforensics.com/downloads/ | 29
2019-07-12 13:04:07 | Download Digital Forensic Software | Foxton Forensics | http://www.foxtonforensics.com/downloads/ | 9
History | 1146 rows
www.foxtonforensics.com

SQLite Database Examiner

- **https://sqlitebrowser.org/**



DB Browser Foe SQLite

Browser Forensics Ebooks

- https://archive.org/details/browser-forensics_202304
- https://archive.org/details/browser-forensics/page/1/mode/2up
- https://archive.org/details/clear-browsing-data-forenscis
- https://archive.org/details/sqlite-data-base-forensics-note

Memory Forensics

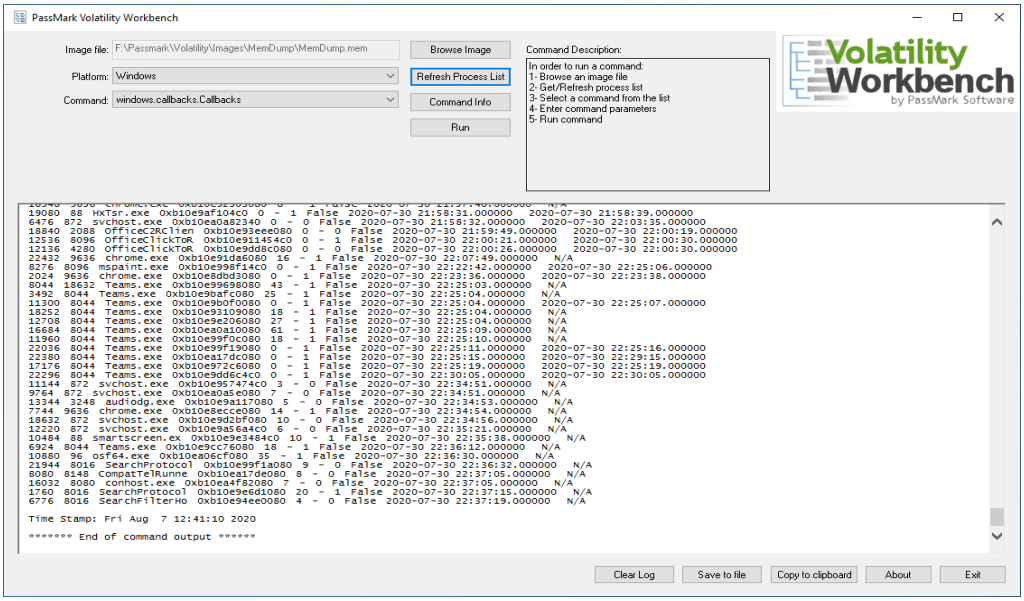
Memory Forensics အတွက်ကို Open Source ရော Commercial Tools တွေမှာရော volatility ကိုပဲအသုံးပြုထားပါတယ်။ GUI Version အသုံးပြုချင်တယ်ဆိုရင် OS Forensics က Free ပေးတဲ့ Volatility Workbench ကို Symbol table packs နဲ့တွဲပြီးအသုံးပြုနိုင်ပါတယ်။

- https://github.com/volatilityfoundation/volatility/releases/tag/2.6.1

hashes.txt 671 Bytes Apr 10, 2024
volatility-2.6.zip 3.99 MB Apr 10, 2024
volatility_2.6_lin64_standalone.zip 14.1 MB Apr 10, 2024
volatility_2.6_mac64_standalone.zip 18.9 MB Apr 10, 2024
volatility_2.6_win64_standalone.zip 14.8 MB Apr 10, 2024
Source code (zip) Dec 18, 2018
Source code (tar.gz) Dec 18, 2018

volatility

- https://www.osforensics.com/tools/volatility-workbench.html



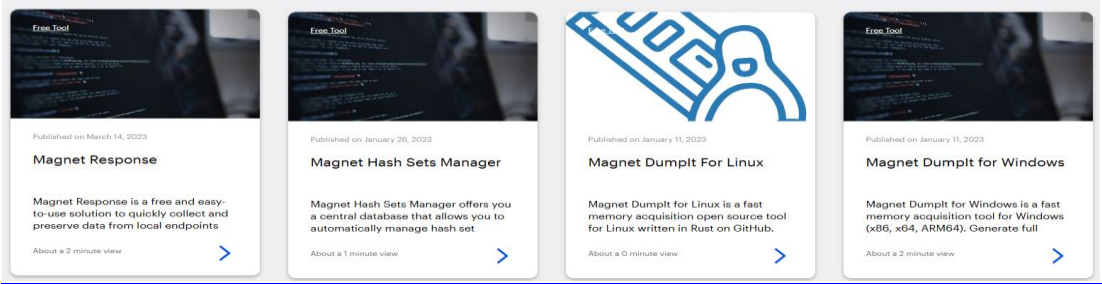
Volatility Workbench

- https://www.sans.org/posters/dfir-memory-forensics/

Commercial Product Free Tools

Commercial Forensics Product ဖြစ်တဲ့ Magnet Forensics ကနေပေးတဲ့ Free Tools တွေကိုအောက်က Link မှာ Download လုပ်ပြီး အသုံးပြုနိုင်ပါတယ်။

- https://www.magnetforensics.com/resource-search-results/?category=free-tool.


Free Tool
Magnet Response
Magnet Response is a free and easy-to-use solution to quickly collect and preserve data from local endpoints
Magnet Hash Sets Manager
Magnet Hash Sets Manager offers you a central database that allows you to automatically manage hash set
Magnet DumpIt For Linux
Magnet DumpIt for Linux is a fast memory acquisition open source tool for Linux written in Rust on GitHub.
Magnet DumpIt for Windows
Magnet DumpIt for Windows is a fast memory acquisition tool for Windows (x86, x64, ARM64). Generate full

Commercial Forensics Product ဖြစ်တဲ့ OS Forensics ကနေပေးတဲ့ Free Tools တွေကိုအောက်က Link မှာ Download လုပ်ပြီး အသုံးပြုနိုင်ပါတယ်။

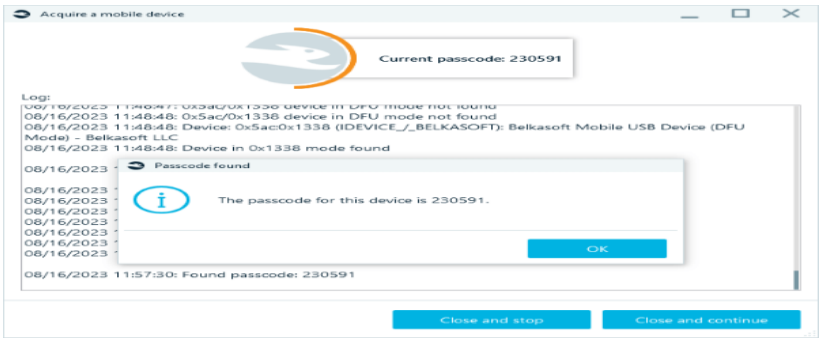
- https://www.osforensics.com/products/index.php
- https://belkasoft.com/belkasoft-triage-is-now-free

OSFMount
Advanced virtual drive manager
OSFMount
OSFMount allows you to mount local disk image files in Windows as a physical disk or a logical drive letter.
LEARN MORE
OSFClone
Self-booting disk cloning tool
OSFClone
OSFClone enables you to create or clone exact raw disk images quickly and independent of the installed operating system.
LEARN MORE
Volatility Workbench
Windows GUI for Volatility memory analysis
Volatility Workbench
Volatility Workbench is a graphical user interface (GUI) for the Volatility command line memory analysis and forensics tool.
LEARN MORE
ImageUSB
Write an image to multiple USB Drives
ImageUSB
ImageUSB is a free utility which lets you write an image concurrently to multiple USB Flash Drives.
LEARN MORE

OS Forensics Free Tools

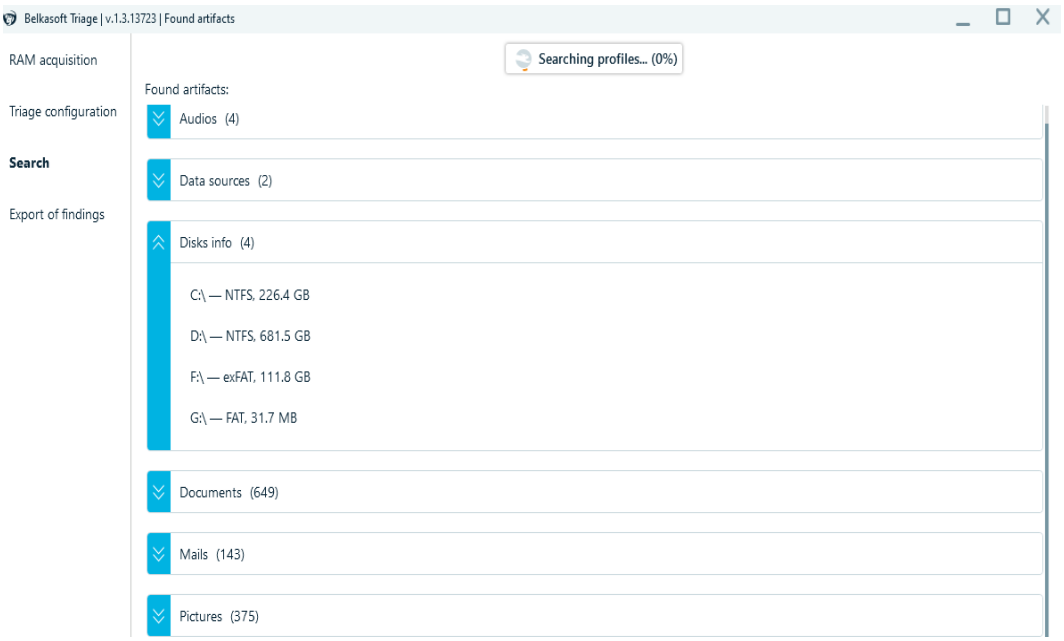
Commercial Forensics Product ဖြစ်တဲ့ Belkasoft ကနေပေးတဲ့ Free Tools တွေကို အောက်က Link မှာ Download လုပ်ပြီး အသုံးပြုနိုင်ပါတယ်။

- https://belkasoft.com/ram-capturer


Acquire a mobile device
Current passcode: 230591
Log:
08/16/2023 11:48:48: 0x5ac/0x1338 device in DFU mode not found
08/16/2023 11:48:48: Device: 0x5ac0x1338 (IDEVICE_/_BELKASOFT): Belkasoft Mobile USB Device (DFU Mode) - Belkasoft LLC
08/16/2023 11:48:48: Device in 0x1338 mode found
Passcode found
The passcode for this device is 230591.
OK
08/16/2023 11:57:30: Found passcode: 230591
Close and stop
Close and continue

Belkasoft Ram Capture

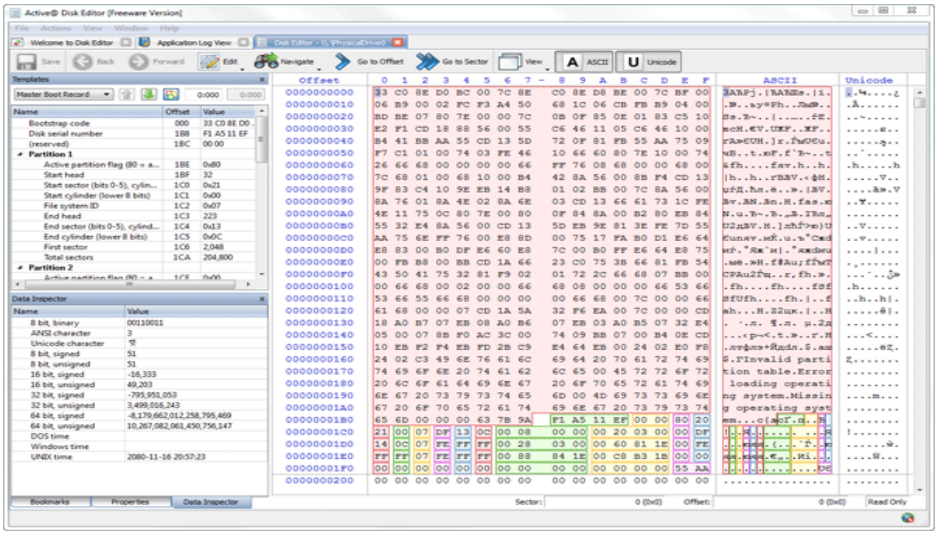
- https://belkasoft.com/belkasoft-triage-is-now-free



Belkasoft Triage

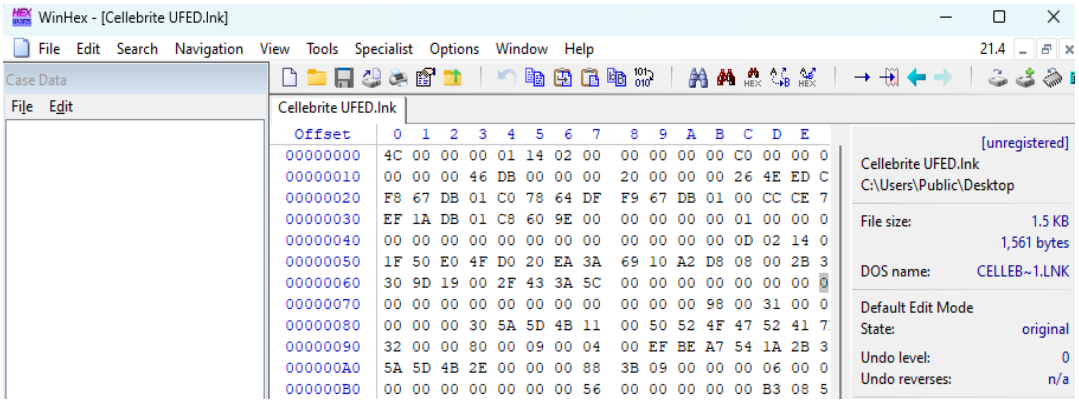
Disk/Hex Editor

- https://www.disk-editor.org/index.html



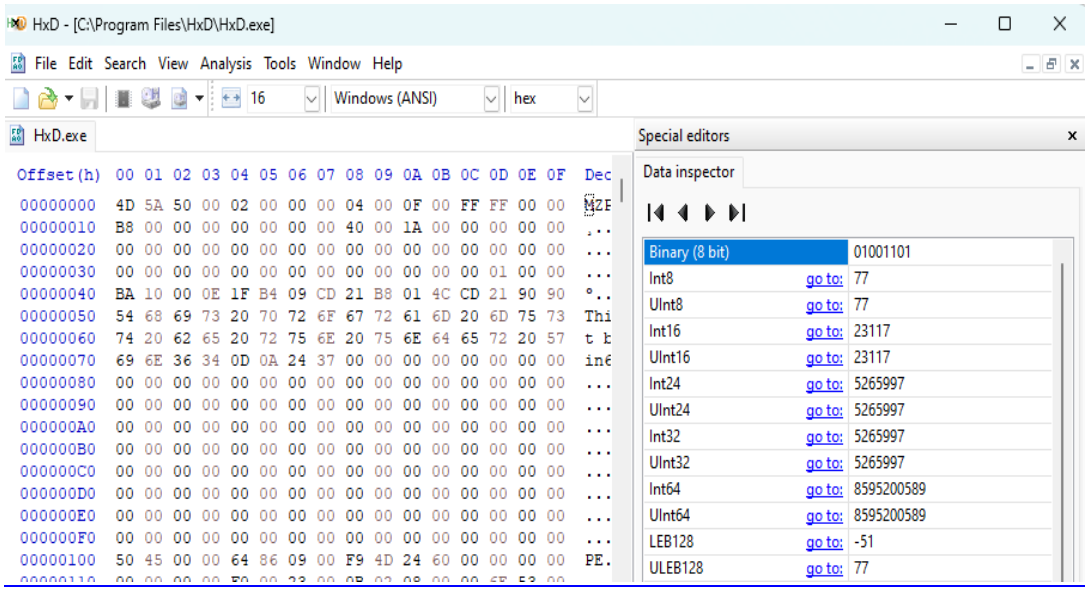
Active Disk Editor

- https://www.x-ways.net/winhex/



Win Hex

- https://mh-nexus.de/en/downloads.php?product=HxD20



HxD

Image Analysis

Image Metdata Analysis အတွက် အောက်က Link တွေကနေ Analysis ပြုလုပ်နိုင်ပါတယ်။ Socaial Media ပေါ်က Photo တွေရဲ့ Metadata ကိုတော့မရနိုင်ပါ။ Socaial Media တွေက

Photo Metadata တွေကိုဖျက်ထားပါတယ်။ Photo ထဲမှာပါတဲ့ အရာတွေ နောက်ခံတွေကိုကြည့်ပြီးသာခွဲခြားနိုင်ပါတယ်။

- https://images.google.com/
- https://www.duplichecker.com/reverse-image-search.php
- https://www.reverseimagesearch.com/
- https://www.reversely.ai/
- https://exiftool.org/forum/index.php?topic=2750.0
- https://exiftool.org/
- https://29a.ch/photo-forensics/#forensic-magnifier

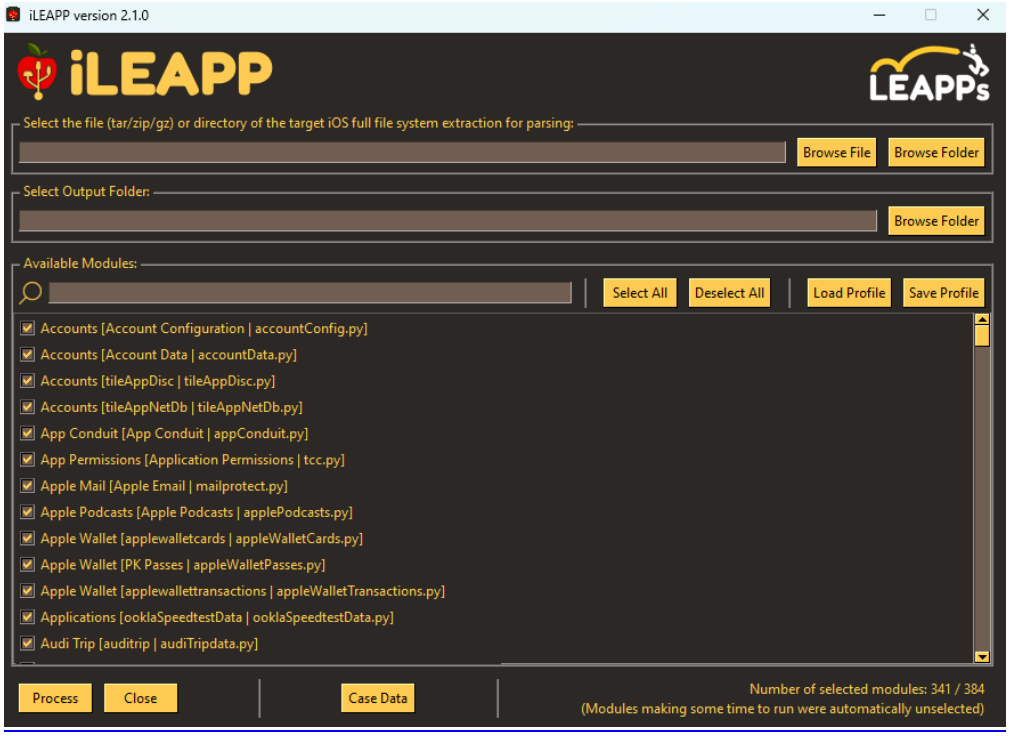
Mobile Forensics

Mobile Forensics အတွက် အောက်မှာပေးထားတဲ့ Link တွေကနေ Download လုပ်ပြီး Analysis ပြုလုပ်နိုင်ပါတယ်။ Mobile Phone ကို Acquire လုပ်နိုင်တဲ့အပေါ်မူတည်ပြီး အဖြေရရှိမှာဖြစ်ပါတယ်။ Logical ပိုင်းပဲရတာများပါတယ်။

- https://github.com/abrignoni/iLEAPP (IOS)

ileapp-v2.1.0-Apple_Silicon.zip	43.8 MB	2 weeks ago
ileapp-v2.1.0-Mac_Intel.zip	45.5 MB	2 weeks ago
ileapp-v2.1.0-Ubuntu.zip	58.6 MB	2 weeks ago
ileapp-v2.1.0-Windows.zip	53.9 MB	2 weeks ago
ileappGUI-v2.1.0-Apple_Silicon.dmg	41.3 MB	2 weeks ago
ileappGUI-v2.1.0-Mac_Intel.dmg	44.9 MB	2 weeks ago
ileappGUI-v2.1.0-Ubuntu.zip	63.4 MB	2 weeks ago
ileappGUI-v2.1.0-Windows.zip	57 MB	2 weeks ago
Source code (zip)		2 weeks ago
Source code (tar.gz)		2 weeks ago

iLEAPP

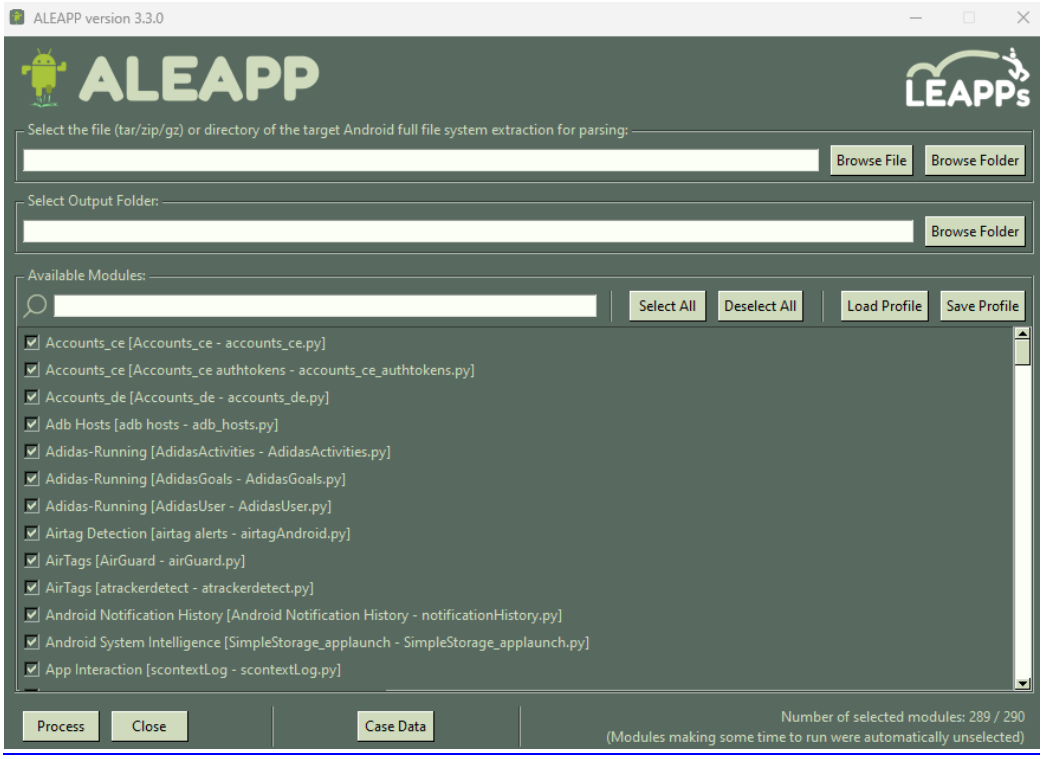

iLEAPP version 2.1.0
iLEAPP
LEAPPs
Select the file (tar/zip/gz) or directory of the target iOS full file system extraction for parsing:
Browse File
Browse Folder
Select Output Folder:
Browse Folder
Available Modules:
Select All
Deselect All
Load Profile
Save Profile
Accounts [Account Configuration | accountConfig.py]
Accounts [Account Data | accountData.py]
Accounts [tileAppDisc | tileAppDisc.py]
Accounts [tileAppNetDb | tileAppNetDb.py]
App Conduit [App Conduit | appConduit.py]
App Permissions [Application Permissions | tcc.py]
Apple Mail [Apple Email | mailprotect.py]
Apple Podcasts [Apple Podcasts | applePodcasts.py]
Apple Wallet [applewalletcards | appleWalletCards.py]
Apple Wallet [PK Passes | appleWalletPasses.py]
Apple Wallet [applewallettransactions | appleWalletTransactions.py]
Applications [ooklaSpeedtestData | ooklaSpeedtestData.py]
Audi Trip [auditrip | audiTripdata.py]
Process
Close
Case Data
Number of selected modules: 341 / 384
(Modules making some time to run were automatically unselected)

iLEAPP

- https://github.com/abrignoni/ALEAPP (Android)

aleapp-v3.3.0-Apple_Silicon.zip	23.4 MB	2 weeks ago
aleapp-v3.3.0-Mac_Intel.zip	25.3 MB	2 weeks ago
aleapp-v3.3.0-Ubuntu.zip	35.5 MB	2 weeks ago
aleapp-v3.3.0-Windows.zip	31.8 MB	2 weeks ago
aleappGUI-v3.3.0-Apple_Silicon.dmg	24.4 MB	2 weeks ago
aleappGUI-v3.3.0-Mac_Intel.dmg	26.2 MB	2 weeks ago
aleappGUI-v3.3.0-Ubuntu.zip	40.3 MB	2 weeks ago
aleappGUI-v3.3.0-Windows.zip	34.9 MB	2 weeks ago
Source code (zip)		2 weeks ago
Source code (tar.gz)		2 weeks ago

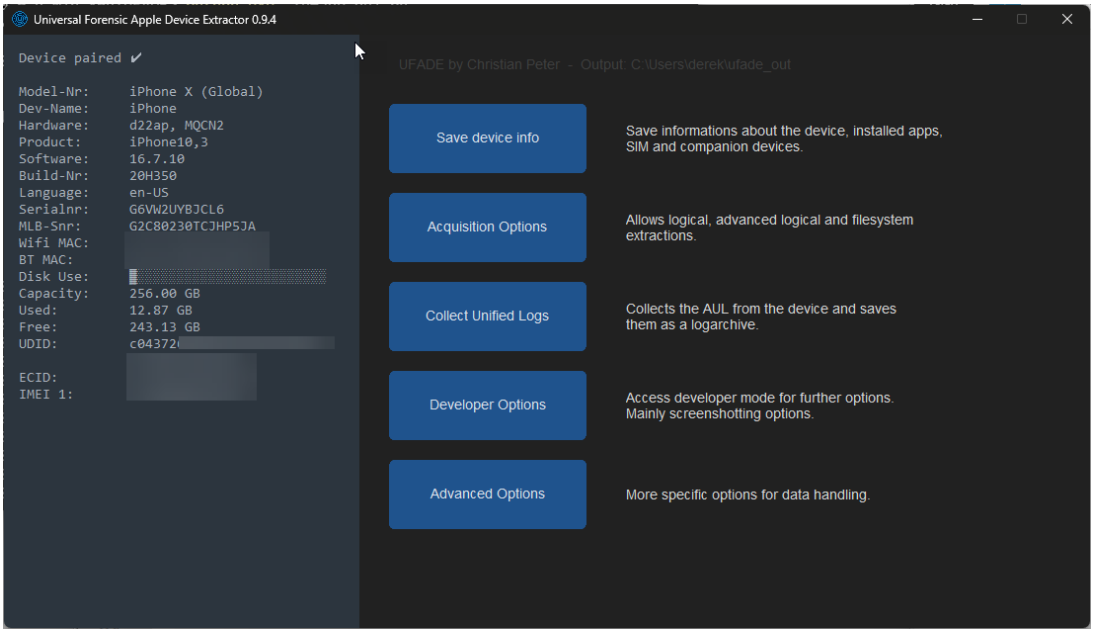
ALEAPP


ALEAPP version 3.3.0
ALEAPP
LEAPPs
Select the file (tar/zip/gz) or directory of the target Android full file system extraction for parsing:
Browse File
Browse Folder
Select Output Folder:
Browse Folder
Available Modules:
Select All
Deselect All
Load Profile
Save Profile
Accounts_ce [Accounts_ce - accounts_ce.py]
Accounts_ce [Accounts_ce authtokens - accounts_ce_authtokens.py]
Accounts_de [Accounts_de - accounts_de.py]
Adb Hosts [adb hosts - adb_hosts.py]
Adidas-Running [AdidasActivities - AdidasActivities.py]
Adidas-Running [AdidasGoals - AdidasGoals.py]
Adidas-Running [AdidasUser - AdidasUser.py]
Airtag Detection [airtag alerts - airtagAndroid.py]
AirTags [AirGuard - airGuard.py]
AirTags [atrackerdetect - atrackerdetect.py]
Android Notification History [Android Notification History - notificationHistory.py]
Android System Intelligence [SimpleStorage_applaunch - SimpleStorage_applaunch.py]
App Interaction [scontextLog - scontextLog.py]
Process
Close
Case Data
Number of selected modules: 289 / 290
(Modules making some time to run were automatically unselected)

ALEAPP

- https://github.com/prosch88/UFADE (IOS)

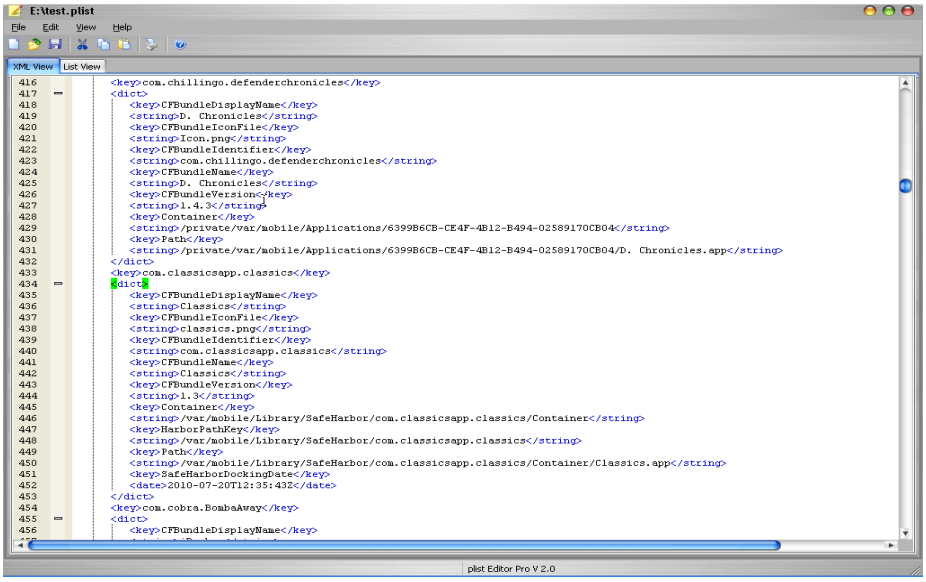
UFADE



UFADE

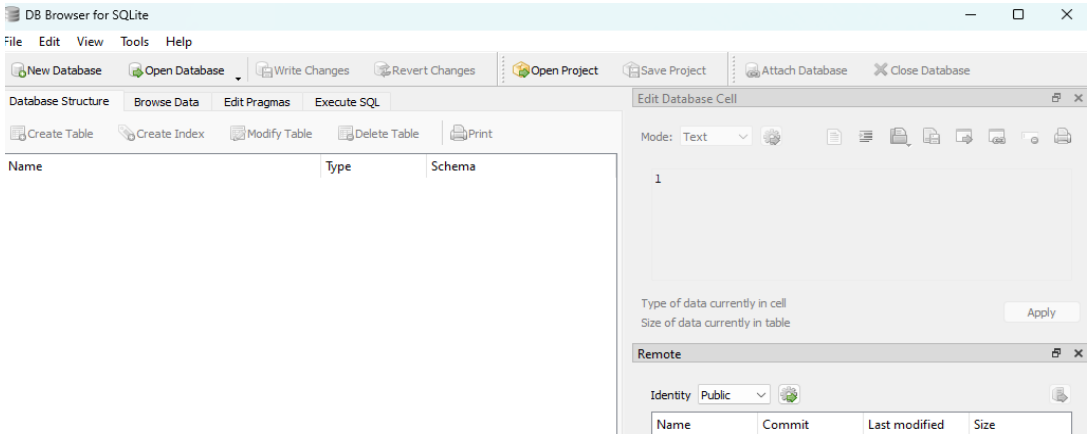
Mobile Forensics (Manual Analysis)

https://www.icopybot.com/plist-editor.htm



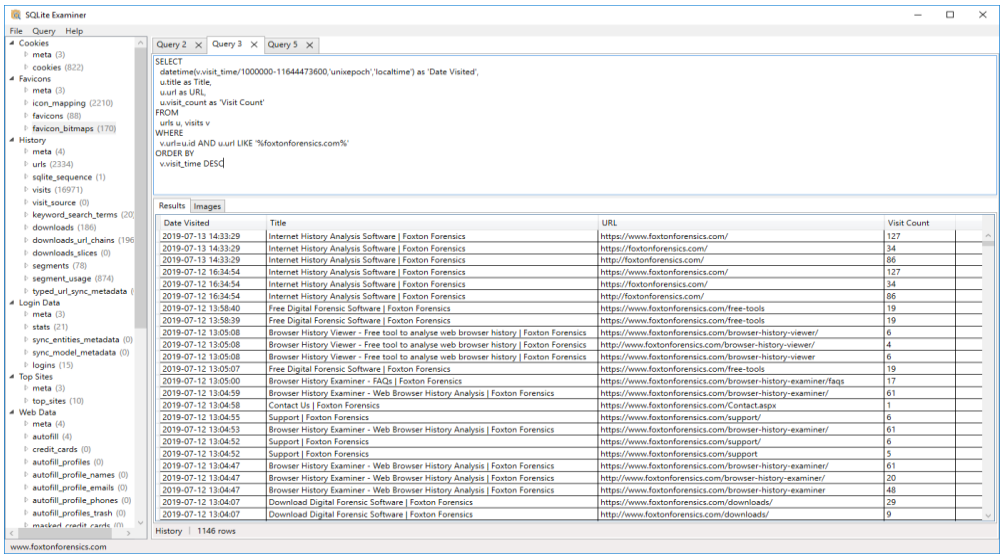
Plist Editor

- https://sqlitebrowser.org/



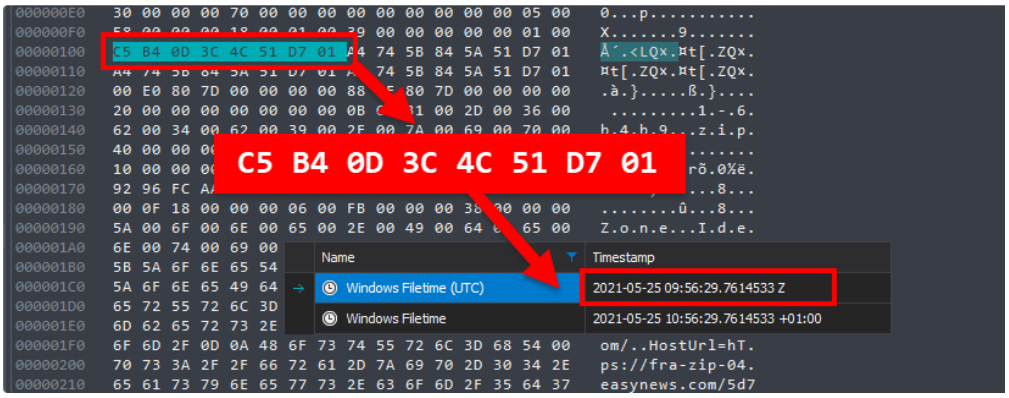
SQLite Browser

- https://www.foxtonforensics.com/sqlite-database-examiner/



SQLite Database Examiner

- https://www.digital-detective.net/dcode/



Timestamp Decoder

Read More About Mobile Forensics

- https://www.sans.org/posters/dfir-advanced-smartphone-forensics/
- https://www.sans.org/posters/android-third-party-apps-forensics/
- https://www.forensicsmyanmar.com/2024/12/mobile-forensics-note-1.html
- https://www.forensicsmyanmar.com/2024/12/mobile-forensics-note-2.html
- https://archive.org/details/chip-off-mobile-forensic
- https://archive.org/details/crash-log-sysdiagnose-log
- https://archive.org/details/how-to-use-mobile-forensics-reader-viewer
- https://archive.org/details/Mobile-Forensics

OSINT

OSINT ဆိုတာဘာလဲ?

OSINT ရဲ့ အရှည်ကောက်က Open Source Intelligence Technique ဖြစ်ပါတယ်။ Internet နဲ့ World Wide Web (WWW) ပေါ်လာတဲ့ အချိန်ကနေစပြီး OSINT ဆိုတာက ပေါ်လာပါတယ်။ OSINT ဆိုတာ Public မှာ တင်တဲ့ သတင်းအချက်အလက်မှန်သမျှ ကို စုဆောင်းတယ်။ အခုဆိုရင် Socail Media တွေပါ ပါလာတာပေါ့။ အဲလို စုဆောင်းတယ် စုဆောင်းလို့ရသမျှသတင်းတွေကို (AI ရော။ လူရော ပေါင်းစပ်ပြီး။ Analysis လုပ်တယ်။)

Analysis လုပ်ပြီးရလာတဲ့ အချက်အလက်တွေကို အခြားတစ်နေရာကနေရလာတဲ့ သတင်း အချက်အလက်တွေနဲ့ ပေါင်းစပ်ပြီး ထပ်ပြီး Analysis ပြုလုပ်တယ်။ နောက်ဆုံးရလာတဲ့ Analysis အဖြေကို Decision လုပ်ပြီး အသုံးချတယ်။ Public ဖြစ်နေတဲ့ Data တွေကို ကောက်ယူတဲ့အတွက် ကုန်ကျမှု သက်သာပါတယ်။

ဘယ်နေရာတွေမှာ အသုံးချလဲ စီးပွားရေး ။ နိုင်ငံရေး။ လူမှုရေး ။ စစ်ရေး အပြင် အခြား Intelligence အပိုင်းတွေအတွက် မဟာဗျူဟာကျကျအသုံးချပါတယ်။ ဒါတွေအပြင် Cyber Security , National Security , စတဲ့ တစ်ဦးတစ်ယောက်ချင်းမှသည် အဖွဲ့အစည်းပိုင်း နိုင်ငံ Level အထိ ဆိုင်ရာအခန်း အလိုက် အသုံးချနိုင်ပါတယ်။

ဥပမာ

စလုံးငွေ တန်ဖိုးအတက်အကျ အလုပ်အကိုင် ပေါ်လစီ စီးပွားရေးနဲ့ပတ်သတ်ပြီး ဥပဒေ တွေ ဘာတွေပြောင်းလဲ သတင်းတွေမှာ ဘာတွေပြောတယ် ဘယ်သူက ဘယ်သူနဲ့တွေ့တယ် တွေ့ပြီးဘာပြောတယ် စတာတွေကို Public ကနေရနိုင်သမျှစုစည်းပြီးရင် ငွေစျေးဘာလို့ကျလဲ ဒီ ဥပဒေ ပေါ်လစီ ပြောင်းရင် ဘာတွေဖြစ်နိုင်မလဲ ဘာလို့ ပြောင်းတာလဲ ဘာကိုရည်ရွယ်ချင်တာလဲ ။ စတာတွေကို Analysis လုပ်တယ်။Analyis လုပ်ပြီးရလာတဲ့ အဖြေကနေ ကိုယ့်ဘက်က လုပ်သင့်တာကို လုပ်မယ်။

ပိုပြီးအကျယ်ချဲ့ရင်တော့ စင်ကာပူထဲမှာ ရင်းနှီးမြှုပ်နှံမှုမှာ ဘာက အများဆုံးလဲ

သူပြိုကျရင် ဘာဖြစ်မလဲ တစ်ခြားဘာတွေပါ လိုက်ပြီးပြိုလဲ မလဲ။

စလုံးနဲ့ စီးပွားရေး အဓိက လုပ်နေတဲ့ အိမ်နီချင်းနိုင်ငံတွေ။ အခြားနိုင်ငံတွေက ဘယ်လိုအခြေအနေရှိလဲ။ သူတို့ တစ်ခုခုဖြစ်ရင် ဖြစ်တဲ့ တစ်ခုကြောင့် စလုံးမှာ ဘာတွေ ထိခိုက်နိုင်လဲ စသည်ဖြင့် Target ထားပြီး လုပ်ဆောင်ရပါတယ်။ ကိုယ့်အတွက် ပိုအကျိုးရှိအောင် ထိရောက်အောင် ချဲ့နိုင်ရင် ချဲ့နိုင်သလောက် ရပါတယ်။ မြန်မာစကားပုံတောင် ရှိပါသေးတယ် ညောင်ဦးကမ်းပါးပြိုတာနဲ့(ဘယ်မြို့ကလဲမသိ) အဲဒီမြို့က နွားမကြီး ခြေကျိုးသလို။ Butterfly Affect ပေါ့။

OSINT မှာ သတင်းစုဆောင်းရုံတင်မဟုတ်ပဲ မှန်မှန်ကန်ကန် Analysis လုပ်ဖို့ ရလာတဲ့ အဖြေကို ထိထိရောက်ရောက် အသုံးချနိုင်ဖို့ ပိုအရေးကြီးပါတယ်။ ဥပမာ ပေးတဲ့ စီးပွားရေးတင်မဟုတ် ။ ကျန်တဲ့ ကိစ္စတွေ နေရာတွေမှာလဲအလားတူပါပဲ။ နေရာစုံ View Point ပေါင်းစုံကနေ ဥပမာ ပေးရရင် တော်တော်ရှည်သွားပါမယ်။ OSINT မှာ AI ကပါသင့်သလောက်ပါဝင်ပေမဲ့ Analysis လုပ်မဲ့လူရဲ့ အရည်အသွေးကလဲ အရေးကြီးပါတယ်။ Analysis လုပ်မဲ့သူက အစွန်း ၂ဖက် လွတ်ရပါတယ်။ Analysis လုပ်မဲ့သူတွေက သက်ဆိုင်ရာ အပိုင်းမှာ expert ဖြစ်ရပါမယ်။ AI ထက် လူတွေက ကောက်ကျစ်တယ် လှည့်ဖျားတတ်တယ်။ မာယာများတယ်။

OSINT အတွက်အရေးကြီးတဲ့ Critical Thinking တွေကတော့ (W6) လုံးဖြစ်တဲ့

(Who, What, Where, When, Why, How)

Who

ကျွန်တော်တို့ A ဆိုတဲ့ သတင်းအချက်အလက်ကို ရရှိလာတဲ့အခါ

A နဲ့ပတ်သတ်ပြီး လက်ရှိမှာ ဘယ်သူ အကျိုးအမြတ်ရမလဲ

A နဲ့ပတ်သတ်ပြီး နောင်တစ်ချိန်မှာ ဘယ်သူ အကျိုးအမြတ်ရမလဲ

A နဲ့ပတ်သတ်ပြီး လက်ရှိမှာ ဘယ်သူ ထိခိုက်နိုင်သလဲ

A နဲ့ပတ်သတ်ပြီး နောင်တစ်ချိန်မှာ ဘယ်သူ ထိခိုက်နိုင်သလဲ

A နဲ့ပတ်သတ်ပြီး အထိခိုက်အများဆုံးက ဘယ်သူဖြစ်နိုင်မလဲ

A နဲ့ပတ်သတ်ပြီး အထိခိုက် အနည်းဆုံးက က ဘယ်သူဖြစ်နိုင်မလဲ

A နဲ့ပတ်သတ်ပြီး ဘယ်သူက ဘယ်နေရာက သတင်းထုတ်ပြန်တာလဲ

A နဲ့ပတ်သတ်ပြီး ဘယ်သူက အဓိက ဆုံးဖြတ်ချက်ပေးတာလဲ

သတင်းအချက် A ထဲမှာ Key Point , Key Person, Key People ကဘာလဲ

A နဲ့ပတ်သတ်ပြီး ပြောဆိုဆွေးနွေးနေတာတွေ ကဘာတွေလဲ

A နဲ့ပတ်သတ်ပြီး ကိုယ်တိုင်ဆုံးဖြတ်နိုင်မလား အခြားသူအကြံယူသင့်သလား

A နဲ့ပတ်သတ်ပြီး အခြား Information Source တွေရှိနိုင်သလား

A နဲ့ပတ်သတ်ပြီး လက်ရှိနေရာမှာ ပုံစံတူ အရင်ကရှိခဲ့ဖူးလား၊

ကမ္ဘာမှာရော A လိုမျိုးပုံစံတူ အရင်ကရော အခုလက်ရှိရောဖြစ်ခဲ့လား

A နဲ့ပတ်သတ်ပြီး ကိုယ်တိုင် ယူဆချက်ပေးလို့ရမလား (အယူအဆကို အစွန်မရောက်စေပဲ)

A ကိုယုံသင့်သလား အသုံးချသင့်သလား

What

A ဆိုတဲ့ သတင်းအချက်အလက် ရရှိလာတဲ့အခါ

အားနည်းချက် အားသာချက် ကဘာလဲ

မှားယွင်းတဲ့ အချက်အလက်တွေပါသလား

Positive or Negative တစ်ဖက်ဖက်ရောက်အောင်ပြောင်းနိုင်မလား

ကိုယ်လိုချင်သလို ရည်ရွယ်ချက်ကောက်ယူနိုင်သလား

အရေးကြီးသလား အရေးမကြီးဘူးလား

အခြားသော ရှုထောင့်ကကြည့်ရင် ဘယ်လိုဖြစ်မလဲ

ဘယ်လိုပြောင်းပြီး မြင်နိုင်သလဲ

ဘယ်လို ခုခံခြေပနိုင်မလဲ

Where

A ဆိုတဲ့ သတင်းအချက်အလက် ရရှိလာတဲ့အခါ

ဘယ်နေရာမှာ ဘယ်အချိန်တွေမှာ ဒီလို ဖြစ်ပျက်ဖူးတာတွေကို မြင်ဖူးကြားဖူးခဲ့သလား

တူညီတဲ့ နေရာ အခြေအနေတွေက ဘယ်နေရာတွေမှာ ဖြစ်ခဲ့လဲ

အဲဒီနေရာကနေ အခြားသော အချက်အလက်တွေ ရနိုင်မလား

ဖြစ်ပျက်ခဲ့တဲ့ အခြေအနေတွေကနေ ဘယ်လိုသင်ခန်းစာ အကြံရယူနိုင်မလဲ

ဘယ်လောက်ထိ ပြဿနာတွေ ဖြစ်ခဲ့လဲ

ဘယ်လို တိုးတက်မှု ဆုတ်ယုတ်မှုတွေ ရှိခဲ့သလဲ ရှိလားနိုင်သလဲ

ဘယ်နေရာကို အကျိုးသက်ရောက်မှု အနည်း-အများဆုံးဖြစ်နိုင်မလဲ

ဘယ်နေရာကနေ စပြီးလုပ်သင့်သလဲ

When

A ဆိုတဲ့ သတင်းအချက်အလက် ရရှိလာတဲ့အခါ

ဘယ်အချိန်တွေမှာ လက်ခံမှု လက်မခံနိုင်မှုတွေ ရှိလာနိုင်သလဲ

ဘယ်အချိန်မှာ ကိုယ့်အတွက် အောင်မြင်မှု ဆုံးရှုံးမှုတွေ ရှိလာနိုင်တာကို သိရှိနိုင်မလဲ

ကိုယ့်အတွက် အရေးကြီးတဲ့ ကိစ္စဘယ်အချိန်မှာ ဖြစ်လာနိုင်မလဲ

ကိုယ့်အတွက် ပြဿနာဖြစ်လာနိုင်မလား

ဘယ်အချိန်မှာ ပြောင်းလဲနိုင်မလဲ

ဘယ်အချိန်မှာ လုပ်သင့်သလဲ

ဘယ် အချိန်ရောက်ရင် အကျိုးသက်ရောက်လာနိုင်မလဲ

ဘယ်အချိန်မှာမှ Action ယူသင့်သလဲ

Why

A ဆိုတဲ့ သတင်းအချက်အလက် ရရှိလာတဲ့အခါ

ဘာအကြောင်းကြောင့် ပြဿနာ အခက်ခဲဖြစ်လာတာလဲ

ဒီအကြောင်းကို အခြားလူတွေကို အသိပေးသင့်သလား

ကိုယ့်အပေါ်သက်ဆိုင်လာနိုင်လား ဒါမှမဟုတ် အခြားသူအပေါ်သက်ရောက်နိုင်မလား

(ဘာလို့လဲ)

ဘာလို့ ဒီလိုတွေဖြစ်နေတာလဲ

ဘာလို့ အဆိုး အကောင်းတွေ ဖြစ်လာတာလဲ

အဆိုး အကောင်းတွေကို ခွင့်ပြုသင့်သလား

ဘယ်လိုအကြောင်းကြောင့်လူတွေကို လွှမ်းမိုးထားနိုင်ရတာလဲ

(ဘာလို့လဲ)

ဘာလို့ ဒီလိုတွေဖြစ်နေတာလဲ

ဘာလို့ အဆိုး အကောင်းတွေ ဖြစ်လာတာလဲ

အဆိုး အကောင်းတွေကို ခွင့်ပြုသင့်သလား

ဘယ်လိုအကြောင်းကြောင့်လူတွေကို လွှမ်းမိုးထားနိုင်ရတာလဲ

ဒီလိုမျိုး အခြေခံ Critical Thinking နဲ့ စဉ်းစားရတဲ့အတွက် နေ့စဉ် လစဉ် နှစ်စဉ် စုဆောင်းထားတဲ့ Information တွေက ပျောက်သွားလို့မရပါဘူး။ စာရွက်ပေါ်မှာ ထားလို့လဲ မရနိုင်ပါဘူး။ ဒါ့ကြောင့် ကိုယ် Target အလိုက် စနစ်တကျ data တွေကို အချိန်မရွေး ကိုယ်လိုချင်တာကို ပြန်ရှာနိုင်အောင် Database အနေနဲ့ ထားသင့်ပါတယ်။

(Fake News ဟုတ် မဟုတ်ကိုလဲ အလားတူခွဲခြားပါသည်။)(intelligence, Psychology Warfare, Counter Intelligence စတာတွေအတွက် အခြေခံကျတဲ့ အတွေးနည်းလမ်းတစ်ခုပါ။)

(လူတစ်ယောက် ကိစ္စတစ်ခု အလုပ်တစ်ခုလုပ်မယ် ပြောမယ်ဆိုမယ်ဆိုရင်လဲ အခြေခံကျတဲ့ Thinking တစ်ခုပါ။)

More About OSINT Tools

- https://start.me/p/nRvKOn/dfm-sm-osint
- https://start.me/p/L1rEYQ/osint4all
- https://start.me/p/DPYPMz/the-ultimate-osint-collection
- https://start.me/p/0Pqbdg/osint-500-tools
- https://www.osintcurio.us/

Digital Forensics Training & Resource

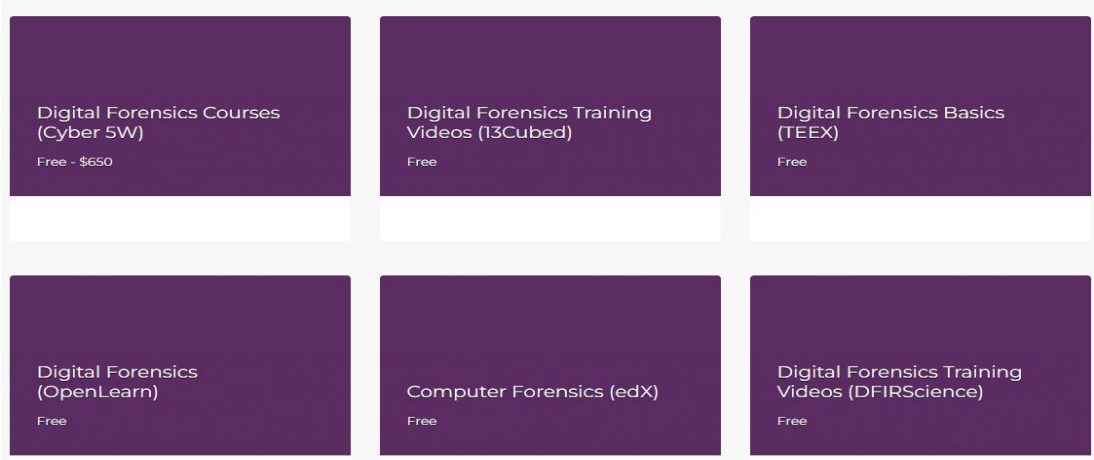
Resource

- https://start.me/p/q6lD4d/digitalforensicsmyanmar
- https://start.me/p/q6mw4Q/forensics
- https://cfreds.nist.gov/
- https://dfirdiva.com/
- https://thisweekin4n6.com/
- https://forensic4cast.com/forensic-4cast-awards/

- https://archive.org/details/@digital_forensics_myanmar

Training

- https://training.dfirdiva.com/listing-category/digital-forensics



Digital Forensics OS

- https://www.sans.org/tools/sift-workstation/
- https://www.parrotsec.org/download/
- https://www.kali.org/get-kali/
- https://tsurugi-linux.org/
- https://www.caine-live.net/

Portable Tools Kit

- https://www.forensicsmyanmar.com/2024/09/bento-dfir-portable-tools-kit.html

Community

- https://discord.com/invite/JUqe9Ek

GUIDE

https://www.swgde.org/

https://www.nist.gov/programs-projects/digital-forensics

အခု PDF မှာ ငွေကုန်တာနည်းနည်းနဲ့ လွယ်လွယ်ကူကူထိထိရောက်ရောက် Free အသုံးပြုနိုင်မဲ့ Resource တွေကိုဖော်ပြထားပါတယ်။ Information တွေအများကြီး စုပြုံပြီး မထည့်ထားပါဘူး။ အရေးကြီးဆုံးက အသစ်အသစ်တွေကို အဆက်မပြတ် လေ့လာပြီး အဆက်မပြတ်ထိတွေ့နေဖို့ပဲဖြစ်ပါတယ်။

Keep Mind Pure !!!

Be Good To Other !!!

Aung Zaw Myo

Digital Forensics Myanmar

www.forensicsmyanmar.com